SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

SOFTWARE DEPLOYMENT IN A DATA COMMUNICATIONS NETWORK

Cross Reference to Related Applications

PRIORITY STATEMENT UNDER 35 U.S.C.119(e) & 37 C.F.R.S1.78. This non-provisional patent applications claims priority based upon the prior U.S. provisional patent application entitled "Software Deployment, Accounting and Personal Portal", application number 60/287,734 filed May 2, 2001, in the name of GONTHIER Jean-Charles, RICHER Eric, HOST Gerald, JODOIN Pierre-Luc, FOURNIER Nicolas, MALTAIS Robert Claude, VAN BUNNINGEN Thomas, HARNOIS Serge, WALLNER Sabine, BRASK Patrik.

Background of Invention

[0001] Technical Field of the Invention

[0002] The present invention relates to data communication networks, and particularly to deployment of software in such networks.

[0003] Description of Related Art

[0004] Not that long ago, to install software on a terminal the software and the terminal had to meet physically, either by bringing the software to the terminal or the terminal to the software. As this obviously is difficult and time consuming in most cases, the growth of computer networks brought ways of distributing software over the network, something that today comes in different guises.

[0005] One method for distributing and downloading software to a computer (or other

kind of terminal) is in a trusted network, where the user simply downloads the software from a file server and installs it himself, usually by activating a self installing program.

[0006] In many cases, however, a company needs to keep track of the number of versions of a certain program that are installed on its computers. This is needed in order to pay license fees to the software providers. In these cases, it is common for the company's network administrators to handle the distribution of data, usually by some kind of remote installation procedure.

[0007] In other cases, a user may download software from a software provider on the Internet and install it on his terminal. This is a variation on the abovementioned theme in that there is no trusted network. Hence the software will, unless it is free, have to be paid for somehow, usually using credit cards.

[0008] Once downloaded, the software may be self-installing so that the user can relax until the installation is finished, or possibly answer some questions as to preferences and so on. These questions may be answered beforehand, for instance when ordering the download of the software, in which case the software may come pre-configured.

[0009] All these instances, however, describe situations in which software is downloaded and installed on a single terminal, although it is of course possible to repeat the procedure from other terminals.

[0010] There is as of today no known procedure that in an easy manner lets a user order the download of software to his own terminal as well as one or more other terminals, have this software automatically configured and installed and then billed for.

[0011] It can therefore be appreciated that there is a need for a solution that overcomes the problems and limitations of the prior art. This invention provides such a solution.

Summary of Invention

[0012] The present invention is directed to a method for software deployment in a data communications network that comprises an Initiator, a Service Provider, and a Peer. The Initiator sends a service request comprising the address of the Peer to the Service Provider that sends an invitation to the Peer. If the Peer accepts the service, it sends an accept service message to the Service Provider that builds the software for the service and distributes it to the Initiator and the Peer. The Initiator and the Peer install the software, and the service is initiated.

[0013] The present invention is further directed to a system for software deployment in a data communications network. The system comprises an Initiator, a Service Provider, and a Peer. The Initiator sends a service request comprising the address of the Peer to the Service Provider, and installs software received from the Service Provider. The Service Provider sends an invitation to the Peer, builds the software for the service, and distributes the software to the Initiator and the Peer. The Peer sends an accept service message from the Peer to the Service Provider, and installs software received from the Service Provider.

[0014] The present invention is further directed to an Initiator of software deployment in a data communications network that further comprises a Service Provider and a Peer. The Initiator comprises a communication unit that sends a service request comprising the address of the Peer to the Service Provider, and receives the software for the service from the Service Provider. The Initiator also comprises a processing unit that installs the software.

[0015] The present invention is further directed to a Peer in software deployment in a data communications network that further comprises an Initiator and a Service Provider. The Peer comprises a communication unit that receives an invitation from the Service Provider, sends an accept service message to the Service Provider, and receives software from the Service Provider. The Peer further comprises a processing unit that installs the software

[0016] The present invention is further directed to a Service Provider for software deployment in a data communications network. The network further comprises an Initiator and a Peer. The Service Provider comprises a communication unit that

receives a service request comprising the address of the Peer from the Initiator, sends an invitation to the Peer, receives an accept service message from the Peer, and distributes the software to the Initiator and the Peer. The Service Provider further comprises a processing unit that builds the software for the service.

Brief Description of Drawings

[0017] A more complete understanding of the present invention may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0018] FIG. 1 depicts a block chart of an exemplary network environment in which the invention may be used;

[0019] FIG. 2 depicts a signal flow chart of a preferred embodiment of the method according to the invention; and

[0020] FIG. 3 depicts a simplified block chart of an exemplary network node.

Detailed Description

[0021] Reference is now made to the Drawings, where Figure 1 depicts a block chart of an exemplary network environment in which the invention may be used. In the network 20, are shown two users, an Initiator 22 and a Peer 26. The Initiator 22 has access to the Internet 10 through an access network 12, while the Peer 26 has a direct connection to the Internet 10. The network 20 further comprises a Service Provider 24, also directly connected to the Internet 10. The Service Provider 24 among other things stores software 25 for the services it provides.

[0022] In an exemplary scenario, the Initiator 22 wishes to share with the Peer 26 the use of a service provided by the Service Provider 24. The service may for example be a game that the Initiator 22 wants to play with the Peer 26, or some kind of communication service such as a telecommunication connection. Neither the Initiator 22 nor the Peer 26 has the proper software to use the service. On the other hand, the Service Provider 24 has the necessary software and is willing to let users partake of this software for a fee that for example may depend on the length

of the utilisation.

[0023] Hereinafter it will be assumed that the Initiator 22 has access to a Portal 14 residing on his own device (not shown). The Portal 14 could however also reside elsewhere in the network 20, as long as the Initiator 22 has access to it. It will also be assumed that the Initiator 22 trusts the Portal 14, that the Initiator 22 is logged on to the Portal 14, and that the Portal 14 has access to or stores information such as for example the identity of the Initiator 22 and security association data (see description of security associations hereinafter). It should be noted that it is not necessary for these assumptions to be true in order for the method according to the invention to work. Using the Portal 14 does however greatly facilitate the working of the method as it automates steps that otherwise would be initiated or performed manually by the Initiator 22.

[0024] Figure 2 depicts a signal flow chart of a preferred embodiment of the method according to the invention. The figure shows, in a network 20, a Service Provider 24 and two users: an Initiator 22 and a Peer 26. It is to be understood however that there may be more than one peer.

[0025] One way of authentication in a network is for two or more entities to have valid security association. This may for instance be a shared secret that no one else knows about. When one entity wants to authenticate another entity it asks for their shared secret and if the response comprises the correct secret, then the other entity is authenticated. An example of such a secret is an encryption key. The first entity draws a random number and sends it to the second entity. Both entities encrypt the number using their shared encryption key. The second entity sends the encrypted number to the first entity that then is able to compare the two encrypted numbers. Encrypting random numbers one way of making sure that a third entity may not learn the shared secret, as the secret is not the number itself nor its encrypted version, but rather the encryption key per se.

[0026] Another example is public key encryption (PKE) where an entity has a private key that only the entity itself knows and a public key that may be known to the entire world. A message encrypted with the public key may only be decrypted with

the corresponding private key, and vice versa. Hence, a message encrypted with the private key may be said to have been signed by the corresponding entity; an electronic signature so to speak. This way an entity that only knows the public key of another entity, may ask that entity for the public keys of other entities. Thus, two entities that previously did not know each other"s public keys may gain knowledge of this, often through an entity they both trust. It will be understood that the invention is not the security associations in themselves; rather it makes use of security associations.

[0027] A person skilled in the art will appreciate that these were merely two examples of security associations and that many other variants exist.

[0028] It is assumed that the Initiator 22 shares a valid security association with the Peer 26 and another valid security association with the Service Provider 24. It is however also possible for the Initiator 22 to negotiate valid security associations using prior art techniques, for example through a so-called broker. The Initiator 22, the Service Provider 24, and the Peer 26 are connected to the network 20, and these three entities may contact one another through the network 20. In case the Initiator 22, the peer 24, or both the Initiator 22 and the Peer 26 are for example human beings, then the network connection is achieved via some sort of device that provides the connection, although in the description hereinafter there may be references to just the entities, which may comprise the user and the device or just the device, as the case may be.

[0029] The Initiator 22 further has his Portal 14 (see Figure 1) activated. This may for example be an Internet portal through which he can use services and browse for information. It is through this Portal 14 that the Initiator 22 may access the Service Provider 24; the Portal 14 may for example provide a link to the Service Provider 24. The Portal 14 itself is however beyond the scope of this invention.

[0030] Turning now to the description of the method according to the invention. In step 202, the Initiator 22 selects a service provided by the Service Provider 24 through the Portal 14, upon which an Interface Request message 204 is sent to the Service Provider 24. This message comprises:

[0031] - The address of the Initiator 22 (a1). This address may for instance be the IP address or a user address, such as for example "John.Doe@JohnDoe.com".

[0032] - A unique identifier for the Interface Request 204 (a2).

[0033] - An indication of the requested service (a3). The indication may also comprise options (a3a) relevant for the presentation of the requested service, such as for example language and display capability.

[0034] - A random number to be used for authentication using the security association (a4).

[0035] - An electronic signature that authenticates the Initiator 22 to the Service Provider 24 (a5).

[0036] The Service Provider 24 then authenticates the Interface Request 204, step 206, and responds with an Interface 208 configured with the options from the Interface Request 204, i.e. having the requested language, display characteristics or whatever was requested in the Interface Request 204. The Interface 208 comprises:

[0037] - The unique identifier from the Interface Request 204 (b1).

[0038] - The requested service interface (b2) with any relevant options (e.g. language).

[0039] - A random value to be used in the subsequent service request 212 (b3).

[0040] - A key to be sent to any peers that the Initiator 22 may wish to contact (b4).

[0041] - An electronic signature that authenticates the Service Provider 24 to the Initiator 22 (b5).

[0042] In step 210, the Initiator 22 prepares and sends, using the Interface 208 to the Service Provider 24 a Service Request 212 comprising:

[0043] - The unique identifier sent in the Interface Request 204 (c1).

[0044] - A unique identifier for the Service Request 212 (c2).

[0045] - An identification of the requested service (c3), normally with any configuration options (c3a), such as for example the kind of connection that is desired with the peers, and particulars of the game that is wanted.

[0046] - An electronic signature that authenticates the Initiator 22 to the Service Provider 24 (c4).

[0047] - A list of peers (in this example only the Peer 26) that the Initiator 22 wishes to share the service with (c5). The message comprises the following information for each peer:

[0048] - The address of the peer (e.g. URL or IP address) (c5a).

[0049] - A notification describing the service that is offered (c5b).

[0050] - An identifier of the Initiator 22 (c53). The identifier is preferably one that the peer can identify without having to consult any other entity.

[0051] - The key from the Interface 208 (c54).

[0052] - An electronic signature that authenticates the Initiator 22 (c55). Once again, it is preferable if the peer can authenticate the Initiator 22 without having to consult any other entity.

[0053] Upon reception of the Service Request 212, the Service Provider 24 registers the options and sends an Invitation 216 to invited peers, i.e. the Peer 26; step 214. The Invitation 216 comprises:

[0054] - A unique identifier for the Invitation 216 (d1).

[0055] - Identification of the offered service with the configuration options selected by the Initiator 22 (d2).

[0056] - An interface to use for the response (d3).

[0057] - The address of the Initiator 22 (d4). If this is not already known, then the Service Provider 24 may use for example a Domain Name Server (DNS) to determine the IP address of the Initiator 22.

[0058] - The identifier of the Initiator 22 (d5).

[0059] - A notification with information about who the Initiator 22 is and what the offered service is (d6).

[0060] - The key provided by the Service Provider 24 in the Interface 208 (d7).

[0061] - An electronic signature authenticating the Initiator 22 to the Peer 26 (d8).

[0062] The Peer 26 may then respond to the Invitation 216. In this example, it is assumed that the Peer 26 accepts the Invitation 216 and therefore responds with an Accept Service message 220 signed using the received key. The message 220 comprises:

[0063] - Options selected by the Peer 26, if any such options were available. These options are left to the Peer's 26 discretion and may for example be display information or language. The Initiator 22, the Service Provider 24, or both the Initiator 22 and the Service Provider 24 may provide these options.

[0064] The Service Provider 24 awaits a sufficient number of responses from the peers before continuing with the next step. What a sufficient number is may depend on several things according on some predefined rule. First, it is sufficient when all the peers have responded. Second, it may be sufficient if at least one peer has responded and a previously set time limit for waiting has expired. Third, it may be sufficient if at least the minimum number of peers needed for the service have accepted. In any case, a predefined minimum number of peers must have accepted the service for the method to go on with the next step. Otherwise, the method may end, perhaps after a predefined time limit, or the Initiator 22 may be informed and possibly offered another service solution.

[0065] The Service Provider 24 now builds the software according to the options, step 222. The Service Provider 24 signs the software so that the users can trust it. The software is also distributed to the Initiator 22 and the Peer 26 in 224 and 226 respectively.

[0066] The Initiator 22 and the Peer 26 then authenticates the software and, if this is

successfully done, the software is installed and automatically started, steps 228 and 230 respectively, and thus the service is initiated, 232. Any signalling needed for the software to communicate with for example other users is specific to the software itself and falls outside the scope of this invention. The software can also be configured to send, possibly periodic, Interim Accounting messages 234 during the service session and a Final Accounting message 238 after the service session. It should be understood that the Interim Accounting messages 234 and the Final Accounting message 238 also may be sent to another accounting entity in the network than the Service Provider 24.

[0067] At 236, one or more users terminate the service session. In this example with only two users, it may well be decided beforehand that the service is terminated for both users as soon as one of them terminates the service. If more users are involved, it may be possible for the remaining users to continue using the service. If the Initiator 22 terminates the service it may be necessary to select a peer who will pay for the continued use of the service.

[0068] The software may be configured to remove itself from the devices once the service has been terminated, step 240 for the Initiator 22 and step 242 for the Peer 26, but it is also possible for the software to remain longer, such as for example a certain number of uses or a certain time period.

[0069] Figure 3 depicts an exemplary network node such as for example a Service Provider 24. The network node 30 comprises a communication unit 31 for communication with other nodes in the network and a processing unit 32 for processing data. The network node 30 also has a network address 33.

[0070] Although several preferred embodiments of the methods, systems and nodes of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.